TÁJÉKOZTATÓ KIADVÁNY

INFORMATIKAI BIZTONSÁGI KORAI FIGYELMEZTETŐRENDSZER (EWS)

A tájékoztató a KÖFOP-2.2.2-VEKOP-16-2016-00001. „KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése” című projekt keretében került kiadásra.

NEMZETI KIBERVÉDELMI INTÉZET
1399 Budapest 62. Pf.: 710/4-2.

Tájékoztató informatikai biztonsági korai figyelmeztetőrendszerhez csatlakozó intézmények számára

(verzió: 6.0)

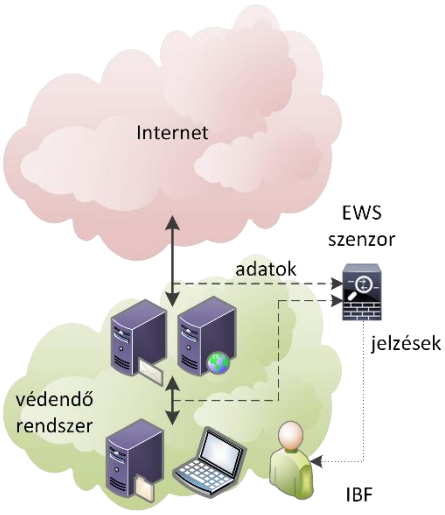
SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

TARTALOM

1 Vezetői összefoglaló

1.1 Mi az az informatikai biztonsági korai figyelmeztetőrendszer (EWS)?

A Kormányzati Eseménykezelő Központ (GovCERT) és a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) feladatait ellátó Nemzeti Kibervédelmi Intézet (NKI) jogszabályi felhatalmazása alapján egy **informatikai biztonsági korai figyelmeztetőrendszer**t (early warning system, továbbiakban: **EWS**) valósít meg. Az EWS az egyes vele egyirányúan összekapcsolt védendő elektronikus információs rendszerek hálózati forgalmának ún. **szenzor**okkal történő passzív elemzésével automatizált módon azonosít kockázatokat, valamint támadásra, visszaélésre vagy ezek kísérletére utaló eseményeket. Az EWS jelzéseket, adatokat és ezekre épülő szolgáltatásokat nyújt az egyes védendő rendszerekre vonatkozóan azok fenntartó intézményeinek kijelölt munkatársai és az NKI számára.



Az EWS kiépítése a KÖFOP-2.2.2-VEKOP-16 projekt keretében 2017-re várható, a védendő rendszerek csatlakoztatására **2018Q4-től** 2021Q4-ig ütemezetten van lehetőség.

Az EWS egyedülálló előnye, hogy a csatlakozó szereplőknek **egységesen magas szintű** kiegészítő védelmet nyújt és annak kihasználásához szükséges oktatást biztosít – mindezt megbízható kormányzati partnertől, központi finanszírozással.

1.2 Miért jó az intézménynek az EWS?

Az EWS rendszer szolgáltatásai a 2013. évi L. törvény (**Ibtv.**) illetve az annak végrehajtásáról szóló 41/2015. (VII. 15.) BM rendelet (továbbiakban: **BMr.**) által előírtan az intézmény által önállóan megvalósításra kerülő védelmi intézkedések nyújtotta biztonságon felüli **kiegészítő intézkedés**ként javítja a csatlakozó intézmény észlelési, felügyeleti, és megfelelőség-ellenőrzési képességét, és ezeken keresztül integritását.

Az EWS segítségével az intézmény számára **hamarabb és nagyobb mértékben válhatnak láthatóvá**, illetve ezáltal kezelhetővé a rendszert érintő támadások (pl. hálózati betörési kísérlet, adatlopás, weboldal rongálás), visszaélések, korrupciós cselekmények (pl. adatszivárogtatás, zsarolási kísérlet) és kockázatok (pl. sérülékeny vagy illetéktelen eszközök és szolgáltatások, lappangó kártevők).

Az EWS csatlakozással az intézménynek csökkennek az incidens kivizsgáláshoz kapcsolódó adminisztratív terhei, mivel (1) a tipikusan átadandó adatok egy része már eleve **elektronikus formá**ban az NKI rendelkezésére áll; valamint (2) az NKI ezen adatok előzetes elemzésével és a védendő rendszer felépítésének ismeretében **célzottabb javaslat**ot tud tenni a még szükséges műszaki adatok begyűjtésére illetve az indokolt védelmi intézkedésekre vonatkozóan.

Az EWS bevezetésékor az NKI szakmai és integritás-tanácsadói képzést biztosít az intézmény kijelölt munkatársai számára térítésmentesen, így járulva hozzá az EWS nyújtotta lehetőségek lehető legnagyobb mértékű kihasználásához. Ezen szakmai továbbképzés, biztonságtudatos és anti-korrupciós szemléletformálás eredményeként a munkatársak jobban hozzá tudnak járulni a védendő rendszerek által kezelt adatvagyon illetve nyújtott szolgáltatások biztonságához, az informatikai biztonsági incidensek kezeléséhez, és a korrupció kockázatának csökkentéséhez.

1.3 Mi az EWS-hez csatlakozás menete?

Az egyes rendszerek fenntartó intézményeinek a csatlakozásra vonatkozó döntést követően általánosságban a következő feladatok végrehajtásáról szükséges intézkedniük:

- a csatlakozási pontok tervét, műszaki/méretezési adatait az NKI-val **jóváhagyatni**;
- a csatlakozás műszaki feltételeit **megteremteni**, illetve a rendszer életciklusa alatt **fenntartani**;
- a műszaki feltételek ellenőrzését, az esetlegesen szükséges EWS eszközök telepítést, illetve az EWS-hez csatlakoztatást az NKI számára **lehetővé tenni** a rendszer életciklusához igazodva, előre egyeztetetten;
- IT illetve integritás-tanácsadó munkatársakat az EWS-hez kapcsolódóan ütemezetten meghirdetendő oktatásokra **delegálni**;
- a rendszer életciklusa alatt bekövetkező változásokat (próbaüzem indulás, élesítés, bővítés, migráció, tulajdonoscsere, kivezetés, stb.) az NKI felé jelezni, valamint azok EWS-t érintő kezelésében (csatlakozási kapacitás bővítés/szűkítés, konfiguráció, stb.) az NKI-val **együttműködni**.

Az intézmény a kiegészítő biztonsági szolgáltatások előnyeit már a csatlakozás kiépítésétől élvezheti a nap 24 órájában.

A dokumentum következő szakaszaiban részletesen bemutatásra kerülnek a rendszerek kialakításánál, továbbfejlesztésénél figyelembe veendő műszaki követelmények [2], az intézmény feladatai a bevezetési [3] és fenntartási [4] időszakban, valamint az EWScsatlakozás intézmény-szempontú hatékonyságát tovább növelő ajánlások [5].

2 EWS csatlakozás műszaki követelmények

Az EWS csatlakozás alapvető műszaki feltétele, hogy az intézmény az NKI-val **egyeztetve** oly módon alakítsa ki, illetve szervezze át a védendő rendszerét, hogy annak legalább az internet felőli biztonsága szempontjából kritikus **hálózati csomópontok**on áthaladó **forgalom másolata** 1 helyen, a lehető legkevesebb, de legfeljebb 2 (nagy rendelkezésreállású rendszerek esetén legfeljebb 4) szabványos hálózati porton titkosítatlanul **átadásra kerüljön**, valamint az azt elemző EWS **szenzorokelhelyezés**e, és a NISZ adatközpontbeli EWS központi alrendszerrel való **összeköttetés**e biztosított legyen.

Az EWS jelzései alapján az intézménynek képesnek kell lennie az esetek **kivizsgálás**ára (incidenskezelés), a jelzésbeli technikai azonosítók (timestamp, IP, port, domain, URL, stb.) alapján az érintett eszközök, szolgáltatások, felhasználók **beazonosítás**ára legalább **2 hónap**ra visszamenőleg megfelelő szervezési illetve **napló**kezelési megoldások kialakításával.

2.1 Hogyan biztosítsam a hálózati forgalom átadását?

Az EWS rendszernek a hálózati forgalom másolatát szükséges átadni szabványos hálózati interfészeken (réz: 100BASE-TX, 1000BASE-T, réz/optika: 1GbE, önállóan vagy LACP aggregálással). A másolás történhet dedikált, lehetőleg valódi passzív vagy fail-open TAP eszközzel[1], vagy indokolt esetben szoftveresen (pl. SSL proxy inspection portja, fizikai/virtuális router/switch monitor portja).

Az EWS rendszer minden **NISZ telephelyen** rendelkezik közvetlen csatlakozási pontokkal, így a forgalom átadása ezen adatközpontokban elérhető portok esetében fizikai vagy virtuális összeköttetéssel történik (patchelés, konfigurálás).

A **NISZ telephelyen kívül**i védendő rendszerek és/vagy portok esetében az NKI-val előzetesen egyeztetendő egyedi kialakítás szükséges, mind az EWS eszközeinek elhelyezésére, mind azok EWS központi rendszerrel való hálózati összeköttetésére vonatkozóan.

2.2 Ha a rendszerem internetelérését a NISZ szolgáltatja, akkor nincs is teendőm?

A védendő rendszerek NISZ által biztosított internetkapcsolatai esetében nem szükséges a védendő rendszerben elemzési pontot kialakítani: a NISZ/NTG internetkijáratain olyan kivezetési lehetőségek kerülnek kialakításra, mely segítségével a elemzési pontot az EWS projekt ki tudja alakítani a védendő rendszer megadott címtartománya (IP/port range) alapján.

Ha a NISZ kijáraton elemezhető forgalom titkosított (pl. HTTPS, SMTPS, VPN), akkor a titkosítás feloldására és a feloldott forgalom elemezhetővé tételére **kiegészítő megoldás** szükséges.

A NISZ kijáraton átmenő forgalom nem feltétlenül egyezik meg a védendő rendszer és az internet közötti tényleges forgalommal, ugyanis a NISZ határvédelmi rendszere kiszűrhet csomagokat, valamint a védendő rendszert más, vele közvetlenül összekapcsolt internetre kötött rendszerek felől is érheti támadás. Mindezek miatt a védendő **rendszeren belül is** ki kell alakítani elemzési ponto(ka)t.

[1] az EWS projekt keretében TAP eszközök korlátozott számban rendelkezésre állnak

2.3 Hogyan oldjam fel a titkosítást?

Alkalmazzon az end-to-end titkosított csatornákat termináló eszközöket, megoldásokat (biztonsági funkcióra dedikált eszközöket [BMr. 3.3.13.3]), mint például:

- saját VPN esetén: a VPN-t végződtetesse külön eszközön, a VPN csatornába terelt forgalmat tükrözze ki[2]
- saját HTTPS/SMTPS/IMAPS vagy más SSL/TLS-sel védett szolgáltatás esetén:
    - az SSL/TLS csatorna kiszolgálón történő végződtetése helyett alkalmazzon **SSL/TLS-képes reverse proxy**-t, így a DMZ-ben már nincs szükség titkosításra, a proxy és a szerver közötti titkosítatlan forgalom TAP-pel elemzés céljára duplikálható[3]
    - amennyiben a kiszolgálón kívüli végződtetés nem megvalósítható, de rendelkezésre áll a szerver titkos kulcsa úgy megfelelő beállítások mellett egy **SSL/TLS decryption** eszköz elő tudja állítani egy TAP által készített titkos forgalom másolata alapján a titkosítatlan forgalmat
- végponti böngészés esetén: alkalmazzon webproxy-ként **SSL/TLS elemzésre és tükrözésre alkalmas új-generációs tűzfalat**[4], ezzel nemcsak az EWS-hez csatlakozást teszi lehetővé, de lényegesen több lehetősége nyílik a böngészés biztonságának növelésére, valamint az internethasználatra vonatkozó házirendek kikényszerítésére[5]

A csatlakozási tervben nyilatkozzon azon titkosított csatornákról, ahol objektív okból nem lehetséges a titkosítás feloldása.

2.4 Hogyan alakítsam ki a kritikus hálózati csomópontokat?

A hozzáférési pontok számának minimalizálása [BMr. 3.3.13.6.2] érdekében biztonsági érzékenység szerint ossza **zónák**ra a rendszerelemeket és erőforrásokat, mint például (a bizalom szintje szerint növekvően):

- internet zóna
- külső DMZ (pl. web/email szerverek/átjárók, távoli elérés)
- intézményi zóna (pl. munkaállomások)
- külső rendszerek zóna (extranet: harmadik fél rendszereivel való kapcsolatok)
- belső DMZ (alkalmazásszerverek)
- korlátozott zóna (pl. kritikus vagy sok adatot kezelő rendszerek, identity management)
- menedzsment zóna (pl. jump hostok, konfiguráció- és naplómenedzsment)

Minden zónának egy meghatározott belépési pontja legyen, amit forgalomelemző tűzfal felügyel (monitoroz és szűr) [BMr. 3.3.13.6.3]. Csak az alapfeladathoz szükséges forgalom

---

[2] ha a VPN csatorna nem dedikált eszközön kerül végződtetésre, akkor akadályba ütközhet minden a csatornába terelt forgalom elemzése, mint pl. a localhost irányú csomagoké

[3] ilyenek pl. a Varnish, nginx, stunnel

[4] ilyenek pl. a ClearTunnel, McAfee Web Gateway, BlueCoat ProxySG, Palo Alto Networks PA-3000/5000/7000, F5 BIG-IP Local Traffic Manager

[5] az EWS projekt keretében korlátozott számban rendelkezésre állnak ilyen eszközök, jelezze igényét

léphessen ki vagy be a zónákból [BMr. 3.3.13.6.3.1.2] [BMr. 3.313.6.4]. A (titkosított) alkalmazásrétegbeli kommunikáció közvetlenül ne, csak átjárókon, lehetőleg alkalmazásrétegbeli proxy szervereken keresztül valósuljon meg [BMr. 3.3.10.4, 3.3.13.6.6] [SP800-53r4 AC-7] például a web, e-mail, DNS, RDP esetében; ahol ez nem kívánatos, ott indokolt a jump hostok használata pl. SSH, DB, IPMI eléréshez.

Ilyen kialakítás mellett az EWS szempontjából leginkább kritikus hálózati csomópontok az internet zónát és külső DMZ-t, valamint az extranet zónát és a belső DMZ-t határoló tűzfalak „belső" oldalai.

2.5 Mik a naplókezelés minimumkövetelményei?

Az EWS által észlelt gyanús események védendő rendszeren belüli kivizsgálhatósága érdekeit figyelembe véve szükséges kialakítani a naplózásba bevont eszközök körét, a naplóbejegyzések információtartalmát és a naplók megőrzési idejét. [BMr. 3.3.12]

A naplózásba minimálisan **bevonandó eszközök** a

- host védelmi eszközök;
- behatolásjelző- és megelőző rendszerek (IDS/IPS);
- VPN vagy más távoli hozzáférés;
- proxy szerverek (web, email, stb.);
- sérülékenységmenedzsment eszközök;
- hitelesítő szerverek;
- tűzfalak, vagy engedélyezési listákat kezelő más hálózati eszközök.

A minimális **megőrzési idő** biztonsági naplók esetében legalább 2 hónap.

Minden naplóbejegyzésnek tartalmaznia kell **időbélyeg**et. A naplózó fizikai/virtuális eszközök rendszeróráit feltétlenül szinkronizálni kell (NTP, lehetőleg NISZ pontosidő szolgáltatás), az időszinkronizáció sikeressége szintén **monitoroz**andó. Azon rendszerek esetében, ahol az időzóna automatikus átállítása (tipikusan CET és CEST között) nem lehetséges ott javasolt az UTC használata.

A naplózás sikerességét folyamatosan **monitorozni** kell.

A monitorozás alatt olyan folyamat értendő, mely proaktív automatikus észlelés alapján olyan jelzést ad, amelyről a probléma elhárítása érdekében intézkedésre kijelölt személy értesül.

3 EWS csatlakozás kialakításához kapcsolódó feladatok

3.1 EWS csatlakozási terv készítése

Az EWS-hez csatlakozó intézmény az NKI-nak jóváhagyásra megküldi a csatlakoztatandó rendszereire vonatkozóan az EWS csatlakozási tervet, mely tartalmazza az alábbiakat:

- az intézmény és a rendszer(ek) kitöltött biztonsági adatlapjait [6.1, 6.2], benne
    - benne a csatlakozás megvalósításának tervezett módját
        - kritikus hálózati csomópontok
        - kivezetők típusai
- **[BMr. 3.3.1.3.1.2]** azonosítsa a rendszer **interfészeit**, határozza meg
    - az interfészek paramétereit (pl. fizikai médium, protokoll, maximális/maximálisan engedélyezett sávszélesség)
    - az átvitt adatok jellegét (protokollok, adattartalom, személyes adatot tartalmaz-e?, tipikus sávszélesség)
- **[BMr. 3.2.5.1.1][SP800-53r4 SA-17]** adja meg a rendszer **infobizt. architektúra** fejlesztői leírását:
    - a biztonsági követelmények alapján szükséges **biztonsági funkcionalitás**, valamint a funkciók **fizikai és logikai eszközök**höz rendelése
    - a biztonsági követelményeknek való megfelelés kimutatása a biztonsági funkciók, **eljárások** és **szolgáltatások** egymásra épülésének bemutatásával
- az EWS csatlakozás folyamatának egykapus kommunikációja érdekében az intézmény által kijelölt operatív kapcsolattartó (pl. vagy a 187/2015. (VII. 13.) Korm. rendelet 8. § szerinti projekt vezetője) elérhetőségeit.

Az egyes pontokhoz benyújtható bármely meglévő, illetve hivatkozható bármely korábban az NKI-hoz benyújtott dokumentum (pl. NEIH OVI űrlap, rendszerterv).

3.2 Műszaki feltételek megvalósítása

A védendő rendszernek az előkészítő tervezés során meghatározott külső vagy zónák közötti interfészeken áthaladó forgalom másolatát az az előkészítő tervezés során meghatározott helyen és módon elérhetővé kell tennie az EWS rendszer szenzorai számára.

- forgalommásoló funkció megvalósítása
    - span/TAP/decryption/proxy csatlakoztatása illetve létesítése, konfigurálása
- hálózati összeköttetés
    - az EWS szenzorok bemeneti interfészeire való kapcsolódás kialakításának támogatása
- nem NISZ telephely esetén felhordó-hálózat és fix sávszélesség biztosítása az EWS szenzorok menedzsment interfészei számára

3.3 Oktatáson való részvétel

- ingyenes oktatásokon való részvétel
    - védendő rendszer technikai személyzete, mint EWS felhasználó
    - védendő intézmény integritás-tanácsadói állománya, mint EWS haszonélvező

3.4 Csatlakozás próbaüzemének támogatása

- együttműködés a kivezetők és szenzorok finomhangolásában
    - nem kivezetendő/vizsgálandó forgalmak azonosítása
    - irreleváns elemzési módok (protokollok) azonosítása
    - jelzési/riasztási szintek hangolása
- intézményi felhasználói felület használatba vétele
    - jogosult személyek regisztrációja
- EWS bevezetésével kapcsolatos esetleges belső szabályozási feladatok végrehajtása
    - szabályzók, szerződések felülvizsgálata

3.5 Adatvédelemmegfelelőségének fenntartása

Az EWS csatlakozáskor különös tekintettel kell lenni azinformációs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.) rendelkezéseinek való megfelelésre, különös tekintettel a rendszerek rendeltetéséből (pl. állampolgárok adatainaknyilvántartása), vagy az intézmény munkáltatói jellegéből (pl. dolgozók bejelentkeztetése) adódóan megjelenő**személyes adatok**–mint például természetes személyneve, azonosítója – védelmére.

A közigazgatási szervek törvényi **feladata elektronikus információs rendszereinek védelme**, nevezetesen gondoskodni az elektronikus információs rendszer eseményeinek nyomon követhetőségéről [Ibtv. 11. § (1) bek.], mely jogalapot teremt az adatkezelő intézménynek a rendszereken tárolt és továbbított személyes adatok biztonsági eseménykezelési célú felhasználására. Az EWS ezen célhoz kötötten támogatja a biztonsági események nyomon követését a műszaki adatok feldolgozásával, de nem az adatok kezelésével –az EWS rendszerben kizárt a személyes adatok felvétele, megváltoztatása, de általában nem biztosított még a személyes adatok beazonosíthatósága sem.

Az**NKI jogosult** az állami és önkormányzati szerveket érintő informatikai biztonsági eseményekhez kapcsolódó, valamint a központosított informatikai és elektronikus hírközlési szolgáltatótól átvett**műszaki, technikai adatok kezelésé**re [Ibtv. 19-20. §, 185/2015. (VII. 13.) Korm. rendelet10-11. §], mely adatok tartalmazhatnak az Infotv. szerint személyes adatnak minősülő adatokat is. Az EWS rendeltetésének nem része, ugyanakkor a felépítésből adódóan elkerülhetetlen a hálózati forgalomban esetlegesen megjelenő személyes adatok feldolgozása, az ebből adódó kockázatok minimalizálására a csatlakozás kialakításakor hálózati csomópontonként az intézmény által jelzett kockázatokkal arányos egyedi **helyettesítő biztonsági intézkedések**[Infotv. 7. §, BMr. 2. szakasz] kerülnek alkalmazásra, mint pl. a feldolgozandó forgalom automatizált előszűrése, kitakarása, potenciálisan személyes adatot tartalmazó naplók megőrzési idejének csökkentése.

Amennyiben az intézmény adatkezelést végez, úgy az EWS szolgáltatásai igénybevételének feltétele lehet az EWS üzemeltetőjének adatfeldolgozói szerződés keretében történő megbízása [Infotv. 10. §], valamint erről az érintettek tájékoztatása.

3.6 Belső szabályozás felülvizsgálata

Az EWS-hez csatlakozás, illetve annak előkészítésére megtett intézkedések indokolttá tehetik egyes szabályzók felülvizsgálatát, különösen:

- Biztonsági eseménykezelési eljárásrend [BMr. 3.1.5.1.]
- Biztonságelemzési eljárásrend [BMr. 3.3.4.1]
- Konfigurációkezelési eljárásrend [BMr. 3.3.6.1]
- Naplózási eljárásrend [BMr. 3.3.12.1]
- Rendszer- és kommunikáció védelmi eljárásrend [BMr. 3.3.13.1]
- belső adatvédelmi és adatbiztonsági szabályzatok [Infotv. 24. §]

4 EWS csatlakozás fenntartásához kapcsolódó feladatok

4.1 EWS üzemeltetési feladatok támogatása

- várható illetve váratlanul bekövetkezett üzemi események (pl. áramszünet, védendő rendszer leállása) jelzése
- amennyiben EWS rendszer részét képező eszköz van az intézmény fizikai felügyelete alatt (pl. saját telephely esetén), akkor az NKI megbízottjai előre egyeztetett belépésének lehetővé tétele

4.2 Változáskezelés

A védendő rendszer felépítését, szolgáltatásait, használatát, kapacitását, a fenntartó intézményt, a kapcsolattartást érintő tervezett vagy várható egyedi vagy tartós változásait **jelezze** az NKI felé az EWS erre a célra kialakított EWS ügyfélkapcsolati felületén keresztül, vagy az NKI felé tett egyéb bejelentéssel összevontan.

Nem várt, vagy akár az NKI által észlelt/jelzett változás esetén **működjön közre** a változás okának, és lehetséges következményeinekazonosításában.

Amennyiben egy változás lényegesen érinti az EWS csatlakozást (pl. annak újratervezését teszi szükségessé), úgy **vonja be** az NKI-t a változás tervezésébe, végrehajtásába – ugyanúgy, mint a csatlakozás kialakításakor.

5 EWS csatlakozás hatékonyságnövelő ajánlások

5.1 Naplókezelés (log management)

Naplókezelés alatt az alkalmazások, operációs rendszerek, szerverek, hálózati és határvédelmi eszközök stb. által előállított eseménynaplók beállítását, gyűjtését, tárolását, elemzését és végül megsemmisítését értjük.

A naplókezelés általános célja, hogy az eseményekkel kapcsolatos információk kellő ideig rendelkezésre álljanak a visszaélések, biztonsági incidensek, vagy üzemzavarok észlelése és kivizsgálása érdekében.

A teljes szervezetre vonatkozóan a naplók (logok) fizikailag elkülönített gyűjtése és archiválása csökkenti a logok véletlen megsemmisülésének illetve rosszindulatú manipulánsának lehetőségét. A folyamatos esemény naplózást egy folyamatos mentési eljárásba javasolt illeszteni. A helyi naplók kisebb időszakra, míg az archivált naplók lehetőleg minél nagyobb, akár a teljes mindenkori működés időszakára terjedjenek ki.

Naplózás sikerességét folyamatosan monitorozni kell, bizonyos szolgáltatások letiltása is indokolt lehet a naplózás helyreállításáig.

A **naplózandó események** körét a napló előállítója szerint csoportosítottuk, kiemelve a minden csoportra érvényeseket:

- Általános
    - Indulás és leállás
    - Biztonsági beállítások változása
    - Felhasználói fiókok illetve csoportok létrehozása/módosítása/törlése
    - Sikeres és sikertelen bejelentkezési kísérletek, kijelentkezések
    - Biztonsági események (pl. limit-túllépés, elégtelen jogosultságok, malware észlelés)
    - Induláskor a naplózó verziója (pl. alkalmazás verzió, OS kernel build, firmware verzió)
- Operációs rendszer
    - Szolgáltatások indítási kísérlete, indulása és leállása
    - Eszközök/adathordozók csatlakoztatása és eltávolítása
    - Rendszeróra változása
- Alkalmazás
    - Felhasználó által kezdeményezett tranzakciók (pl. űrlap kitöltés, e-mail küldés, HTTP kérés) és azok sikeressége
    - Üzletmenet szempontjából kritikus elemhez történő hozzáférés
    - Kivételek, abnormális leállás
- Hálózati eszközök (router, switch)
    - Biztonsági szűrők által megakadályozott forgalom (pl. fw rule, ARP spoof)

    - Csatlakoztatott eszközök (link-state, switchport, MAC)
    - Címkiosztás és -fordítás (DHCP, NAT)
- Határvédelmi eszközök (firewall, IDS/IPS)
    - Biztonsági szűrők által megakadályozott forgalom (pl. fw rule, IP/domain blacklist)
    - Ismerten gyanús forgalom (pl. port-scan, graylist, SQLi)
    - Kiugróan magas forgalom (burst, DDoS)
- Egyéb elemek
    - Biztonsági vonatkozásaik mérlegelése alapján a log-kezelésbe indokolt lehet bevonni további elemeket is:
    - Hálózati ki-/beviteli eszközök (pl. nyomtatók, kamerák)
    - Hálózati üzembiztonsági eszközök (pl. UPS, PDU, AC)
    - Távfelügyeleti interfészek (pl. IPMI/iLO/DRAC/AMT, IP-KVM, VNC)
    - Fizikai biztonsági rendszerek (pl. beléptetők, átlépési pontok, mozgásérzékelők)

További naplókezelési tanácsokat talál az alábbi **hivatkozások**on:

- NIST
  Guide to Computer Security Log Management (Special Publication 800-92)
  http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
- Microsoft TechNet
  Biztonsági események naplózása – gyakorlati tanácsok
  http://technet.microsoft.com/hu-hu/library/cc778162.aspx
- Cisco
  Network Security Policy: Best Practices White Paper
  http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html

5.2 Hálózathasználati házirendek

Nemcsak a rendszer biztonságát növeli, de a kezelendő fals jelzések számát is csökkenti a forgalomáramlási szabályok kialakítása [BMr. 3.3.13.6.3] a nemkívánatos hálózati forgalom csökkentése érdekében, mint például:

- alapfeladattal, közszolgálattal össze nem egyeztethető célú felhasználás korlátozása
    - fájlcserélők;
    - videómegosztók, streaming szolgáltatások;
    - aggresszív, szexuális, illegális tartalmak;
    - nem-intézményi VPN;
- magáncélú felhasználás szabályozása (ellenjavallat, korlátozás).

Hasonlóan előnyös a felügyelni kívánt forgalom meg nem figyelt csatornákon keresztüli áramlásának korlátozása, elsősorban adminisztratív intézkedésekkel:

- mobilnet, WiFi korlátozása;
- mobil eszközök (pl. pendrive, okostelefon, laptop) csatlakoztatásának szabályozása;
- felhasználói VPN, külső proxy szerverek, és anonimizáló szolgáltatások (pl. TOR) használatának korlátozása.

5.3 Határvédelmi eszközök beállítása

A határvédelmi eszközök irányába menő, potenciálisan kártékonyként azonosított hálózati csomagok olyan EWS jelzést eredményezhetnek, amelyek nem jelentenek veszélyt, ha a határvédelmi eszköz azokat nem továbbítja. A továbbítás tényére vonatkozó információ nem feltétlenül áll rendelkezésre (pl. egy a határvédelmi eszköz másik oldalán található felügyelt csomópont forgalmának elemzésével), és így feleslegesen vezethet kivizsgálás kezdeményezéséhez.

Amennyiben a kivezető tűzfal mögött kerül elhelyezésre, úgy a tűzfal lehetőleg a megfelelő ICMP válaszcsomaggal jelezze az elutasított forgalmat a későbbi elemzések támogatása, hamis pozitív jelzések azonosítása érdekében.

6 Mellékletek

6.1 Védendő intézmény adatlap (minta)

Kategória	Megnevezés	Adat	Megjegyzés
Alapadatok	Intézmény neve	*Pelda Hatterintezmeny*	
	jogelőd vagy korábbi nevek	*Előd Közalapítvány*	*jogutódlással megszűnt*
	felügyelő minisztérium	*PM*	
Informatikai biztonságért felelős személy (IBF/CISO)	neve	*Biztos Ferenc*	
	telefon	*+36 1 555-5555*	
	mobil	*+36 30 555-5555*	
	email	*ibf@pelda.gov.hu*	
Biztonsági besorolás	Ibtv. hatálya alá esik	*igen*	*biztonsági szint: 3*
	nb. védelem alá esik	*igen*	
	nemzeti létfontosságú rendszerelem (KIV)	*nem*	
Saját online jelenlét	hivatalos honlap(ok)	*www.pelda.gov.hu, www.projekt.hu*	
	allokált publikus domainnevek	*pelda.gov.hu, *.pelda.gov.hu, elod.gov.hu, projekt.hu*	
	allokált publikus fix IP címek/címtartományok	*84.206.1.64/27, 195.10.20.30*	
	Internet, email, DNS, VPN, VoIP, stb. szolgáltatók	*NISZ, Telekom*	*Telekom csak másodlagos DNS*

6.2 Védendő rendszer adatlap (minta)

Kategória	Megnevezés	Adat	Megjegyzés
Alapadatok	**rendszer neve**	*Uveggolyo Nyilvantarto (UNy)*	
	jogszabály(ok)	*42/2042. (V/35.) PM rendelet*	
Biztonsági osztály	**bizalmasság**	*3*	*jelenleg: 2*
	sértetlenség	*3*	*jelenleg: 1*
	rendelkezésre állás	*3*	*elérve: 2015.*
IT felelős	**neve**	*Szaki Szabolcs*	
	telefon	*+36 1 555-5555*	
	mobil	*+36 30 555-5555*	
	email	*it@pelda.gov.hu*	
Internet kapcsolat	**elérhető felületek**	*https://www.pelda.gov.hu/uny, 84.206.1.65:8081 (API), 84.206.1.66:2222 (SSH)*	
	kijáratok	*84.206.1.66:10001-65000*	*szerverek frissítésére szolgáló kijárat (NAT)*
	fizikai interfész és előfizetett sávszélesség	*84.206.1.64/27: 1GbE/30 Mbps*	*kihelyezett NISZ CE routeren, nem redundáns*
	átlagos és csúcsterhelés	*0.5Mbps/12Mbps*	*2015. május hónap alapján*
	titkosítás aránya	*SSL/TLS: 60%, SSH: <1%*	
Külső rendszer kapcsolatok	**függőségek**	*NISZ DNS, NISZ KAÜ*	
	összeköttetések	*MÁK KSzR (feltöltés/letöltés)*	
Elsődleges kritikus hálózati csomópont	**összekötött zónák**	*az Internet-zónabeli SSL/TLS terheléselosztó és a DMZ-beli webszerverek között*	
	fizikai interfészek	*2 × 1 GbE (LACP trönk)*	
	átlagos és csúcsterhelés	*0.4Mbps/10Mbps*	
	EWS kivezető típusa	*fizikai TAP*	
Másodlagos kritikus hálózati csomópont	**összekötött zónák**	*a DMZ-beli szerverek és az Internet-zónabeli NAT-oló router*	
	fizikai interfészek	*1 GbE*	
	átlagos és csúcsterhelés	*0.2Mbps/10Mbps*	
	EWS kivezető típusa	*SSL/TLS proxy*	

Jegyzetek